Dr.K.V.Durgaprasad, S.Vasundhara / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.1810-1816

# ELLIPTIC CURVE CRYPTOGRAPHY

**Dr.K.V.Durgaprasad**
Prof.of Mathematics(Rtd)
OsmaniaUniversity
(For Women)Shaikpet,Hyderabad.

**S.Vasundhara**
Asst.Prof of Mathematics
G.Narayanamma Institute of Technology&science

## ABSTRACT:

**The paper gives an introduction to Elliptic curve cryptography and how it is used in the implementation of digital signature and key agreement algorithms. The paper discusses the implementation of ECC over finite fields, prime fields and binary fields. It also gives an overview of ECC implementation on different coordinate systems called the projective coordinate systems. The paper also discusses the basics of prime and binary field arithmetic.**

## INTRODUCTION:

The use of elliptic curves in connection with cryptography was a first proposed independently by Neal Koblitz and victor Miller in 1985.

An Elliptic curve like any curve in two dimensional coordinate geometry , is made up of points (x,y) satisfying an equation. The coordinates of point as well as the coefficients of a field($2^m$)
public key cryptosystem: asymmetric cryptography, also called public key cryptography, is relatively newfield. It was invented by Diffie-Hellman in 1976.The idea behind a public-key cryptography is that it might be possible to find a cryptosystem where it is computationally infeasible to determine $d_k$ given $e_k$.If so , then the encryption rule is a public key which could be public just as our telephone number or e-mail id.Under this situation,say A wants to send a secret message to B. Then A will use the encryption rule $e_k$ that is made public by B,to encrypt the secret message and send the encrypted message to B through insecure channel.Since,it is computationally infeasible to determine $d_k$ given $e_k$,only B can decrypt the cipher text to get the plain text .The main advantage of a public key cryptosystem is that A can send an encrypted message to B,without any prior communication of a secret key,by using the public encryption rule $e_k$. B will be the only person that can decrypt the cipher text,using the decryption rule$d_k$ which is called the private key**.**

Symmetric and asymmetric systems have their own strengths and weaknesses. In particular, asymmetric systems are vulnerable in different ways such as through impersonation, and are much slower in execution than are symmetric systems. However ,they particular benefits and importantly can work together with symmetric systems to create cryptographic mechanisms that are elegant and sufficient and can give an extremely high level of security.

In 1977, a year Ron Rivest,Adi Shamir and leonard Adleman and is probably the most widely used public key cryptosysytem.It was patented in the US in 1983

**RSA Cryptosystem**

Let n be a product of two distinct primes p and q.Let P=C=$Z_n$.Let us define K={(n,p,q,e,d):ed≡1 (mod$\emptyset(n)$},where $\emptyset(n), called\ euler\ f$unction, is the number of positive integers less than n which are relatively prime to n.For each K=(n,p,q,e,d), we define $e_k^{(x)}$=$x^e$(modn) and $d_k^y$=$y^d$(modn),where x,y ∈ $Z_n$.The values n and e are public and the valuesp,q and d are used as public key.
Now we will verify that this really forms a public –key cryptosystem . Suppose A wants to send a secret message to B using the public-key of B.For that first we will give algorithm for the generation of keys for B.

**B's algorithm to construct keys:**

.Generate two distinct large primes p and q, each roughly of same size.
.compute n=pq and $\emptyset(n) = (p-1)(q-1)$.
Select a random integer e with 1<e<$\emptyset(n)$,such that gcd(e, $\emptyset(n)) = 1$
.use the extended Euclidean algorithm to find the integer d,1<d<$\emptyset(n)$,,such that ed≡1mod($\emptyset(n)$,).
.use public key is n and e and his private key is p,q and d.
A's algorithm for encryption:
.Obtain B's public-key(n,e)
.represent the message as an integer m in the interval[0,n-1].
.compute c≡ $m^e$9modn).
Send the cipher text c to B.
**B's algorithm to decrypt the message:**
To obtain the plain text messagem,B uses his private key d to get m≡ $c^d$(modn).

## DISCRETE LOGARITHMIC PROBLEM=

Consider the multiplicative group($Z_p^*$,$p^*$), where p is a prime. Let g be a generator of the group ,i.e, successive powers of g generate all elements of the group .So

$g^1$ modp,$g^2$mod p……..$g^{p-1}$ modp
Is a re-arrangement of the integers in $Z_p^*$
Let x be an element in {0,1,2, …………..p-2}.The function
Y=$g^x$ ( modp)Is referred to a modular exponentiation with base g and modulus p.
The inverse operation is expressed as x=$log_g^y$ (modp)
And is referred to as the discrete logarithm. It involves computing x given the values of p,g and y∈ $Z_p^*$

**Example Discrete logarithm in ($Z_p^*, 29^*$) with g=2**

| y | $log_2^y$(mod29) |
|---|---|
| 1 | 28 |
| 2 | 1 |
| 3 | 5 |
| 4 | 2 |
| 5 | 22 |
| 6 | 6 |
| 7 | 12 |
| 8 | 3 |
| 9 | 10 |
| 10 | 23 |
| 11 | 25 |
| 12 | 7 |
| 13 | 18 |
| 14 | 13 |
| 15 | 27 |
| 16 | 4 |
| 17 | 21 |
| 18 | 11 |
| 19 | 9 |
| 20 | 24 |
| 21 | 17 |
| 22 | 26 |
| 23 | 20 |
| 24 | 8 |
| 25 | 16 |
| 26 | 19 |
| 27 | 15 |
| 28 | 14 |

From the above problem it gives value of x given p&g means that
$2^7$mod29=12 i.e $log_2^{12}$ $= 7$
Similarly $2^{21}$mod29=17i.e $log_{29}^{17}$=21 and so on
Example let p=131,g=2

| y | $log_2^y$(mod29) |
|---|---|
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| 4 | 16 |
| 5 | 32 |
| 6 | 64 |
| 7 | 128 |
| 8 | 125 |
| 9 | 119 |
| 10 | 107 |
| 11 | 83 |
| 12 | 35 |
| 13 | 70 |
| 14 | 9 |
| 15 | 18 |
| 16 | 36 |
| 17 | 72 |

**The discrete logarithmic problem is**
**$2^{17}$(mod 131)=72,**
***i.*  e $log_2^{72}$ (mod 131)=17,$2^{11}$(mod131)=83**
**i.e $log_2^{83}$mod131)=11**

## DIFFEE-HELLMAN KEY EXCHANGE

Assume that both A and B know the base g amd modulus p in advance they then participate in the following sequence of steps.

A

B

$g^a$ modp→

Choose a and compute $g^a$modp

Choose b
Compute $g^b$mod p

← $g^b$modp

Compute($g^b$modp)$^a$
=$g^{ab}$modp

Compute ($g^a$ modp)$^b$
=$g^{ab}$modp

← Common secret=$g^{ab}$modp→

Example let p=131 and g=2
Let the random number chosen by A be 24.so,her partial key is $2^{24}$mod 131≡46.
Let the random number chosen by B be 17.So,his partial key is $2^{17}mod131 \equiv 72$
After receiving B's partial key ,A computes the shared secret as $72^{24}$mod131≡13.
After receiving A's partial key ,B computes the shared secret as $46^{17}$ mod131≡13

## ELLIPTIC CURVE DISCRETE LOGARITHMIC PROBLEM:

Elliptic Curve is a set of solutions (x, y) to an equation of the form y2=x3+ax+b where 4a3+27b2≠0, together with a point at infinity denoted O. Elliptic Curve originally developed to measure circumference of an ellipse and now have been proposed for applications in cryptography due to their group law and because so far no sub exponential attack on their discrete logarithm problem.

Cryptography based on elliptic curves depends on arithmetic involving the points of the curve.

Definition: An elliptic curve E over a field K is defined by following equation which is called Weiestress equation.

E:y2+a1xy+a3y=x3+a2x2+a4x+a6

y2=x3+ax+b is the simplified version of the Weiestress equation.

Figure 1. Group law on elliptic curve y2=fx over R

Group Law

The definition of Group Law is where the chord-and-tangent rule of adding two points in the curve to give third point which reflects across the x-axis. It is this group that is used in

the construction of elliptic curve cryptographic systems.

Closure, Inverse, Commutative, Identity and Associativity are conditions that the set and operation must satisfy to be qualify as a group which also known as group axioms.

**Addition Formulae:**

Let P1=(x1,y1) and P2=(x2,y2) be non-inverses. Then P1+P2=(x3,y3)

Scalar multiplication:

Scalar multiplication is repeated group addition: cP=P+…+P (c times)where c is an integer

The Elliptic Curve Discrete Logarithm Problem (ECDLP):

The security of all ECC schemes are depends on the hardness of the elliptic curve discrete logarithm problem.

Problem: Given two points W, G find s such that W=sG

The elliptic curve parameters for cryptographic schemes should be carefully chosen with appropriate cryptographic restriction in order to resist all known attacks on the ECDLP which is believed to take exponential time. O(sqrtr) time, where r is the order of W By comparison, factoring and ordinary discrete logarithms can be solved in...

**Example of an Elliptic Curve Group over Fp :**

**As a very small example, consider an elliptic curve over the field $F_{23}$. With a = 1 and b = 0, the elliptic curve equation is $y^2 = x^3 + x$. The point (9,5) satisfies this equation since:**

**$y^2$ mod p = $x^3$ + x mod p**

**25 mod 23 = 729 + 9 mod 23**

**25 mod 23 = 738 mod 23**

**2 = 2**

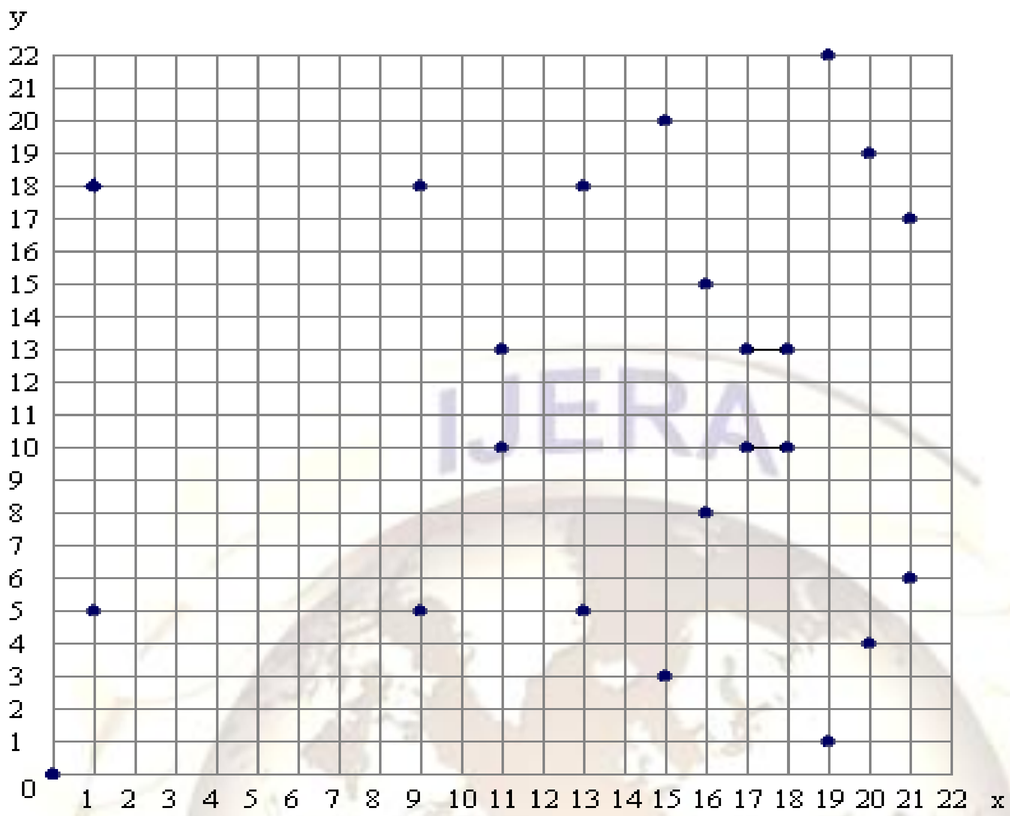
**The 23 points which satisfy this equation are:**

**(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5)**

**(13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10)**

**(18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)**

**These points may be graphed as below:**




**Elliptic curve equation: $y^2 = x^3 + x$ over $F_{23}$**

**Note that there is two points for every x value. Even though the graph seems random, there is still symmetry about y = 11.5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. Over the field of $F_{23}$, the negative components in the y-values are taken modulo 23, resulting in a positive number as a difference from 23. Here -P = ($x_P$, ($-y_P$ Mod 23))**

**Elliptic Curve Groups over F2m** **$F_2m$:**

There are finitely many points on a curve over $F_2m$ .

Elements of the field $F_2m$ are m-bit strings. The rules for arithmetic in $F_2m$ can be defined by either polynomial representation or by optimal normal basis representation. Since $F_2m$ operates on bit strings, computers can perform arithmetic in this field very efficiently.

An elliptic curve with the underlying field $F_2m$ is formed by choosing the elements a and b within $F_2m$ (the only condition is that b is not 0). As a result of the field $F_2m$ having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation:

$$y^2 + xy = x^3 + ax^2 + b$$

The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over $F_2m$ (where x and y are elements of $F_2m$ ). An elliptic curve group over $F_2m$ consists of the points on the corresponding elliptic curve, together with a point at infinity, O. There are finitely many points on such an elliptic curve.

4.1 An Example of an Elliptic Curve Group over F2m

As a very small example, consider the field $F_24$, defined by using polynomial representation with the irreducible polynomial $f(x) = x^4 + x + 1$.

The element g = (0010) is a generator for the field . The powers of g are:

$g^0 = (0001)$ $g^1 = (0010)$ $g^2 = (0100)$ $g^3 = (1000)$ $g^4 = (0011)$ $g^5 = (0110)$

$g^6 = (1100)$ $g^7 = (1011)$ $g^8 = (0101)$ $g^9 = (1010)$ $g^{10} = (0111)$ $g^{11} = (1110)$

$g^{12} = (1111)$ $g^{13} = (1101)$ $g^{14} = (1001)$ $g^{15} = (0001)$

In a true cryptographic application, the parameter m must be large enough to preclude the efficient generation of such a table otherwise the cryptosystem can be broken. In today's practice, m = 160 is a suitable choice. The table allows the use of generator notation ($g^e$) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without reference to the irreducible polynomial

$$f(x) = x^4 + x + 1.$$

Consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. Here $a = g^4$ and $b = g^0 =1$. The point $(g^5, g^3)$ satisfies this equation over $F_2m$ :

$$y^2 + xy = x^3 + g^4x^2 + 1$$

$$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$$

$$g^6 + g^8 = g^{15} + g^{14} + 1$$

$$(1100) + (0101) = (0001) + (1001) + (0001)$$

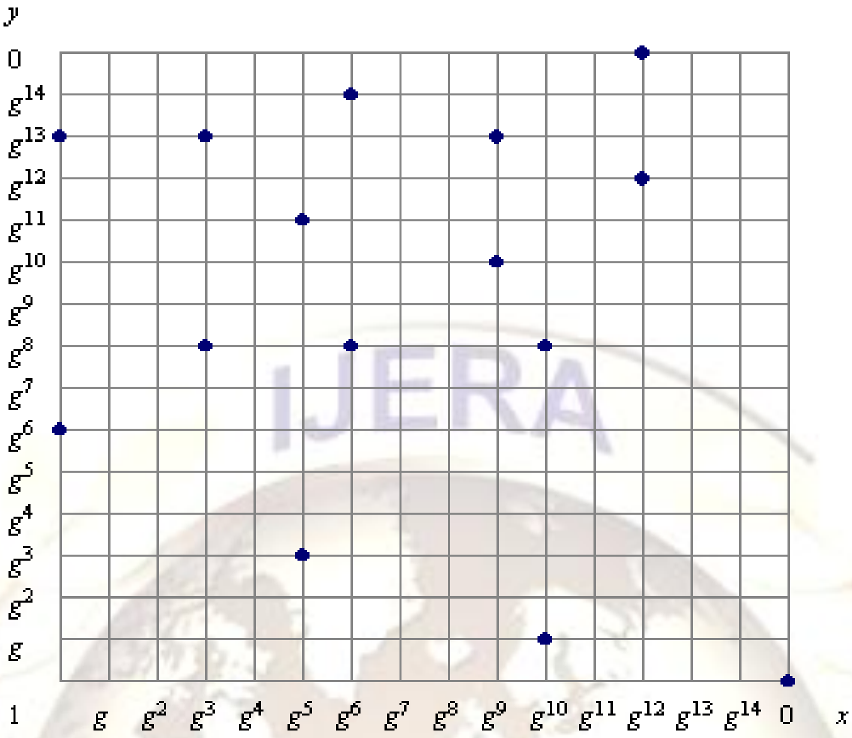
$$(1001) = (1001)$$

The fifteen points which satisfy this equation are:

$(1, g^{13})$ $(g^3, g^{13})$ $(g^5, g^{11})$ $(g^6, g^{14})$ $(g^9, g^{13})$ $(g^{10}, g^8)$ $(g^{12}, g^{12})$

$(1, g^6)$ $(g^3, g^8)$ $(g^5, g^3)$ $(g^6, g^8)$ $(g^9, g^{10})$ $(g^{10}, g)$ $(g^{12}, 0)$ $(0, 1)$

These points are graphed below:




$$y^2 + xy = x^3 + g^4x^2 + 1 \text{ over } F_{2^4}$$

## 5.0 Elliptic Curve groups and The Discrete Logarithm Problem

At the foundation of every cryptosystem is a hard mathematical problem that is computationally infeasible to solve. The discrete logarithm problem is the basis for the security of many cryptosystems including the Elliptic Curve Cryptosystem. More specifically, the ECC relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).
Recall that we examined two geometrically defined operations over certain elliptic curve groups. These two operations were point addition and point doubling. By selecting a point in a elliptic curve group, one can double it to obtain the point 2P. After that, one can add the point P to the point 2P to obtain the point 3P. The determination of a point nP in this manner is referred to as Scalar Multiplication of a point.
The ECDLP is based upon the intractability of scalar multiplication products.

In the multiplicative group Zp*, the discrete logarithm problem is: given elements r and q of the group, and a prime p, find a number k such that r = qk mod p. If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number that Pk = Q; k is called the discrete logarithm of Q to the base P.
When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithm problem is:
given points P and Q in the group, find a number k such that Pk = Q

Example:

In the elliptic curve group defined by

$y^2 = x^3 + 9x + 17$ over $F_{23}$,

What is the discrete logarithm k of Q = (4,5) to the base P = (16,5)?

One (naïve) way to find k is to compute multiples of P until Q is found. The first few multiples of P are:

P = (16,5) 2P = (20,20) 3P = (14,14) 4P = (19,20) 5P = (13,10) 6P = (7,3) 7P = (8,7) 8P = (12,17) 9P = (4,5)

Since 9P = (4,5) = Q, the discrete logarithm of Q to the base P is k = 9.

In a real application, k would be large enough such that it would be infeasible to determine k in this manner.
What is the discrete logarithm of Q(-0.35,2.39) to the base P(-1.65,-2.79) in the elliptic curve group $y^2 = x^3 - 5x + 4$ over real numbers ?